

Exhibit J

Exhibit A

**Infringement of U.S. Patent No. 9,373,122
by Zoho Corporation Pvt. Ltd. and Zoho Corporation**

Subject to ongoing discovery and investigation, Liberty Peak Ventures, LLC (“LPV”) identifies the following accused instrumentality of Zoho Corporation Pvt. Ltd. and Zoho Corporation (collectively, “ZOHO”):

Zoho Vault Applications. This includes:

Zoho Vault Password Manager & AutoFill setting

Zoho Vault for (Windows, macOS, Android, and iOS device platforms)

Zoho Vault Mobile – for iOS (iPhone, iPad, Apple Watch) and Android

Zoho Vault Extensions for the browsers: Chrome, Firefox, Safari, Edge, Vivaldi, Brave

Zoho Vault (Standard, Professional, and Enterprise versions)

Zoho Applications that include Zoho Vault:

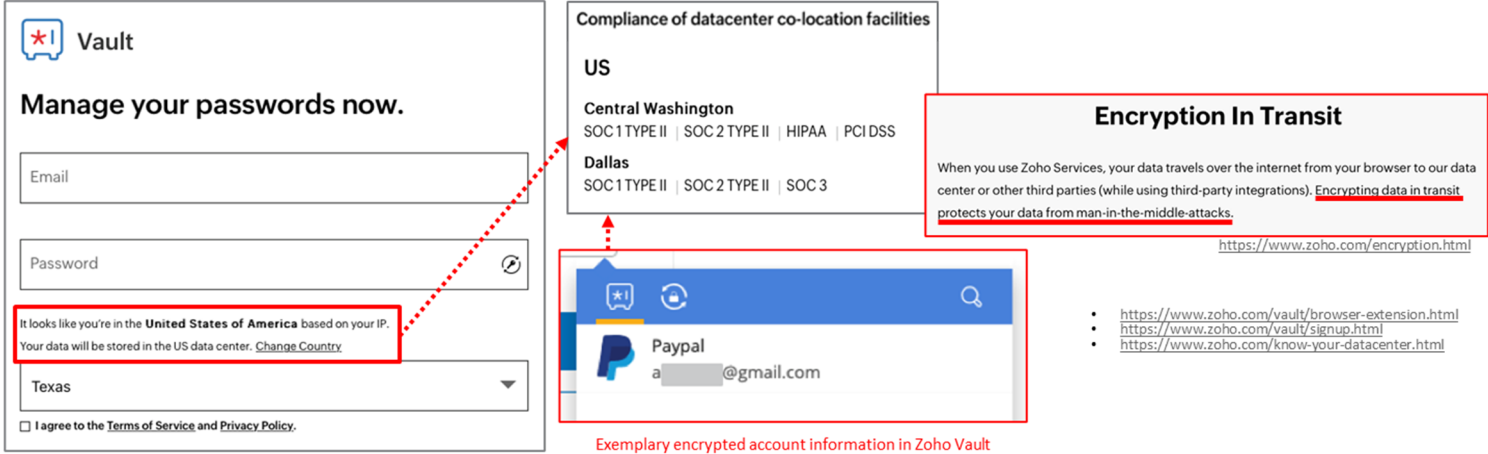
Wavebox Desktop App

Zoho Projects

LPV’s identification of this accused instrumentality is based on publicly available information. LPV has not yet received any discovery from ZOHO. LPV reserves its right to seek discovery regarding other products and services offered by ZOHO, and to identify additional accused instrumentalities based on that discovery and further investigation.

Subject to ongoing discovery and investigation, LPV contends, pursuant to the Court’s April 4, 2022 Order that each element of each infringed claim is found within each accused instrumentality as shown below:

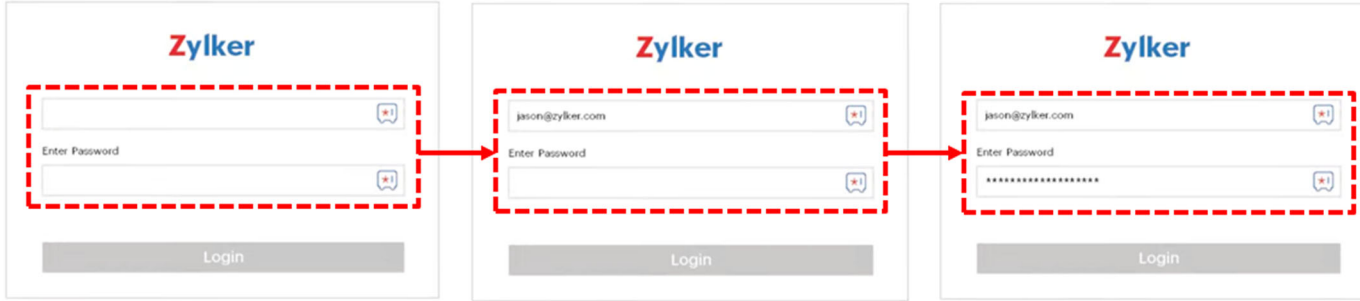
Claim Language	ZOHO Vault Applications
<p>1. A method comprising:</p>	<p>Zoho provides software implementation of a method.</p> <div data-bbox="478 272 1371 578" style="border: 2px solid black; padding: 10px;"> <p>What is a password management software?</p> <p>To facilitate and automate the password management best practices, individuals and businesses need software that can help them securely store, share, and manage passwords. They can also bolster the overall security, privacy, and productivity in their day-to-day operations.</p> </div> <ul style="list-style-type: none"> • https://www.zoho.com/vault/enterprise-password-manager-guide.html
<p>detecting, at a browser toolbar of a computer system, a request from a web service to obtain account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder;</p>	<p>Zoho detects and automatically populates fields on a website with PayPal information (“account information”) that is used to conduct, for example, a payment transaction.</p> <div data-bbox="464 711 1938 1268"> </div> <p>Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription)</p> <p>https://www.zoho.com/vault/features/access-websites-with-a-single-click-browser-extension.html</p> <div data-bbox="1276 1292 1719 1416" style="border: 1px solid black; padding: 5px;"> <p>Forget all your passwords</p> <p>Log in to your favorite websites from Vault using our browser extension, and you'll never have to type out your login information again.</p> </div> <ul style="list-style-type: none"> • Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription) • https://www.zoho.com/vault/features/access-websites-with-a-single-click-browser-extension.html

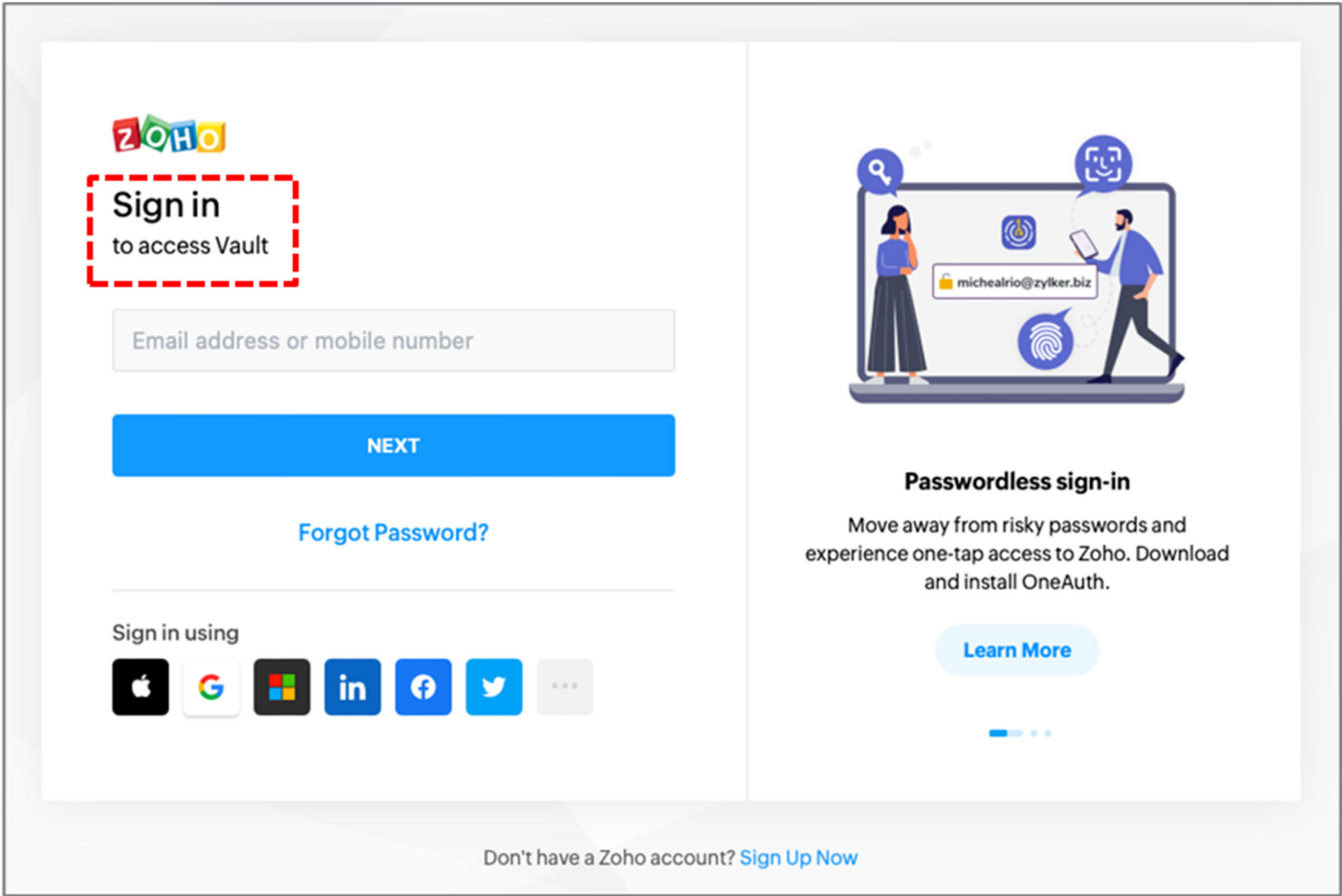
Claim Language	ZOHO Vault Applications
<p>sending, by the browser toolbar, a request for the account information to a secure database that stores the account information;</p>	<p>Zoho sends a request to access user account information that is stored securely in the cloud in an encrypted form. The Zoho app syncs with the cloud periodically to store a local version of the encrypted data.</p> <p>Browser Extension</p> <p>To make password management and logon seamless, Zoho Vault gives you the option to <u>securely synchronize passwords across browsers using browser extensions</u>. These extensions help you <u>auto-fill passwords and automatically log in to websites</u>. You can also add secrets to Zoho Vault directly from the extension whenever you use a new account in any web application. Once deployed, your browser extension will be able to perform most of your password management operations, with Zoho Vault running in the background.</p>  <p>Encryption In Transit</p> <p>When you use Zoho Services, your data travels over the internet from your browser to our data center or other third parties (while using third-party integrations). <u>Encrypting data in transit</u> protects your data from man-in-the-middle-attacks.</p> <p>https://www.zoho.com/encryption.html</p> <ul style="list-style-type: none"> https://www.zoho.com/vault/browser-extension.html https://www.zoho.com/vault/signup.html https://www.zoho.com/know-your-datacenter.html <p>Exemplary encrypted account information in Zoho Vault</p> <ul style="list-style-type: none"> https://www.zoho.com/encryption.html https://www.zoho.com/vault/browser-extension.html https://www.zoho.com/vault/signup.html https://www.zoho.com/know-your-datacenter.html

Claim Language	ZOHO Vault Applications
<p>decrypting, by the browser toolbar, encrypted data received from the secure database, wherein the encrypted data includes the account information, wherein the decrypting is performed using an encryption key maintained by the browser toolbar and inaccessible outside of the browser toolbar;</p>	<p>Zoho uses a locally generated and stored encryption key to decrypt user account data.</p> <div data-bbox="472 300 1249 690"> <h3>Data Security and Privacy</h3> <p>Zoho Vault leverages the host-proof-hosting technique, a secure, proven mechanism which has found wide acceptance after undergoing extensive testing by security experts. Host-proof-hosting is based on the idea of <u>hosting sensitive data in an encrypted form to ensure clients can only access and manage their data using a master password which is never transmitted to the server.</u> The server is limited to persisting and retrieving only the encrypted data the browser forwards it, and <u>can never actually access the sensitive data in its plain form. All encryption and decryption takes place in the client side (browser).</u></p> <p>All passwords and other sensitive data that users store in Zoho Vault remain completely private and can only be viewed by the respective user. <u>All user data gets encrypted and decrypted in the browser with the user's Zoho Vault master password, and only the encrypted data gets stored in Zoho's servers.</u> The user's master password is never stored anywhere by Zoho Vault, meaning even Zoho can never access your data.</p> </div> <div data-bbox="1270 251 1984 690"> <p>"Master password" is used to encrypt/decrypt a local encryption key that is used to decrypt user account data.</p> <p>When users in your organization sign up with Zoho Vault, an RSA Public-Private Key pair is generated for each of them. <u>The user's private key is encrypted using their master password and stored in Zoho Vault's database.</u></p> <p>When the user tries to share a password, <u>the user's private key (stored in encrypted form in the database) is retrieved and decrypted using the user's master password.</u> The encrypted Org Key that the administrator has shared with the user is then retrieved. The encrypted org key is decrypted using the user's Private Key. The password to be shared is now encrypted using the Org Key.</p> <p>Local, device level decryption of user account data</p> </div> <h3>Password Sharing - Flow of Events</h3> <p>Let's use an example. Assume a user John is the admin in the organization and he wants to share one of his existing passwords with, say, five other org users, Maria, Jason, Tracy, Roger, and Amanda.</p> <ul style="list-style-type: none"> ★ Because the password being shared is owned by John, it is <u>stored in Zoho Vault after being encrypted using John's master password</u> ★ When sharing is initiated, the password is <u>decrypted using John's master password</u> <p>https://www.zoho.com/vault/security.html</p> <h3>How do the users retrieve this password?</h3> <ul style="list-style-type: none"> ★ <u>The users decrypt their respective RSA private keys using their respective master passwords</u> <p>https://www.zoho.com/vault/security.html</p>

Claim Language	ZOHO Vault Applications
<p>securely storing the account information at the browser toolbar; and</p>	<p>The decrypted/raw user data (“account information”) is stored in the temporary memory (RAM) as a CPU process memory.</p> <div data-bbox="468 284 1083 467" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>The second, slightly more complicated method uses two passwords: a traditional account password for logging in and a master password for the vault encryption. The user must enter both to see the data. The account password is treated like a normal account password and compared to its hash, while the vault password is <u>used only for decryption on the client side. The password managers that use this strategy are Trend Micro, Zoho Vault, and PassPack.</u></p> </div> <div data-bbox="1108 284 1999 479" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Browser Extension</p> <p>To make password management and logon seamless, Zoho Vault gives you the option to securely synchronize passwords across browsers using browser extensions. These extensions help you auto-fill passwords and automatically log in to websites. You can also add secrets to Zoho Vault directly from the extension whenever you use a new account in any web application. Once deployed, your browser extension will be able to perform most of your password management operations, <u>with Zoho Vault running in the background.</u></p> </div> <div data-bbox="478 506 846 906" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Source: Zoho user on Google Chrome</p> </div> <div data-bbox="871 641 1999 776" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Zoho Vault - Like others, this has both an account password and an encryption password. The account password and username are transmitted in plaintext, so the server stores some password-related information for the account password. When the encryption password is entered, the server sends an encrypted JSON dict with one value: the timestamp of the last account login. The master key is generated from the encryption password using PBKDF2 with 1,000 iterations. <u>The master key is used to decrypt the JSON - if it succeeds, the password is deemed correct, and the server sends the rest of the encrypted vault. Decryption happens client-side in the browser.</u></p> </div> <div data-bbox="1354 506 1600 535" style="color: red;"> <p>CPU process memory</p> </div> <div data-bbox="1024 868 1428 909" style="margin-top: 20px;"> <ul style="list-style-type: none"> • https://www.zoho.com/vault/browser-extension.html • https://www.osti.gov/servlets/purl/1257179 </div> <div data-bbox="508 974 1239 1089" style="margin-top: 20px;"> <ul style="list-style-type: none"> • Source: Zoho user on Google Chrome • https://www.zoho.com/vault/browser-extension.html • https://www.osti.gov/servlets/purl/1257179 </div>

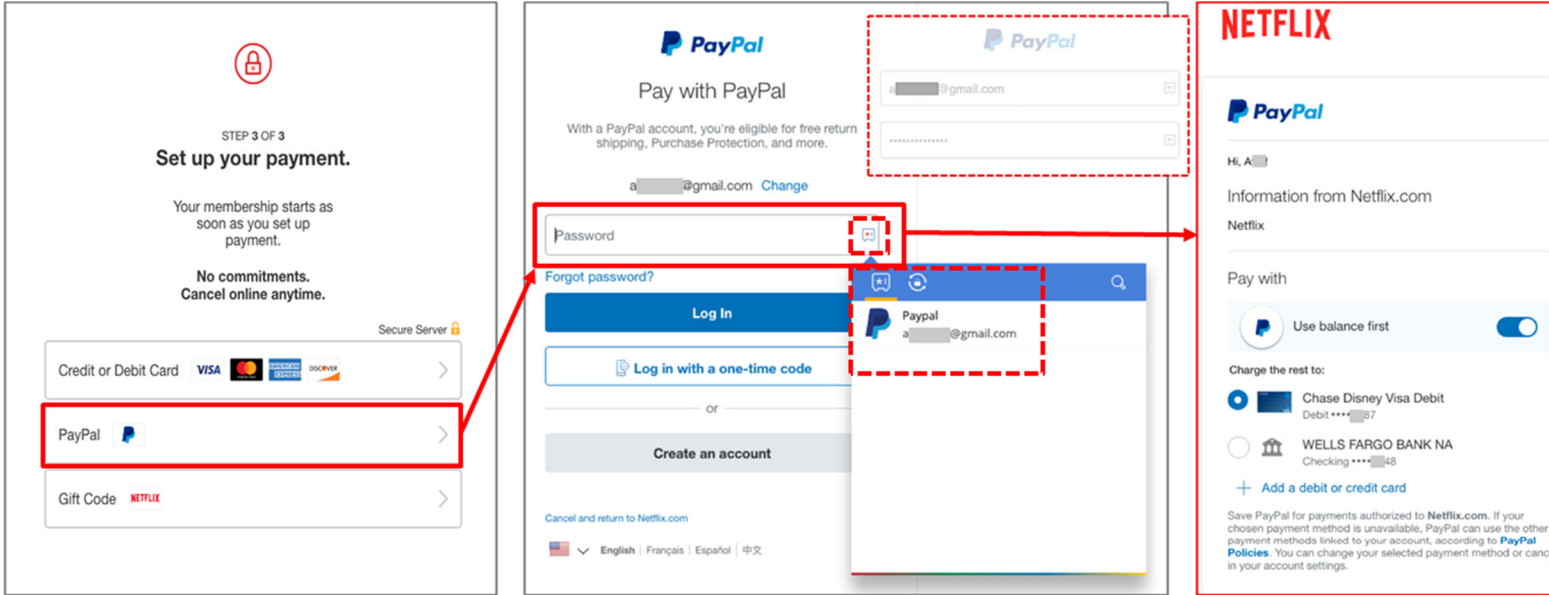
Claim Language	ZOHO Vault Applications
<p>removing the stored account information from the browser toolbar after completion of the transaction.</p>	<p>Raw account information is only available in Zoho until the transaction is complete, otherwise only the encrypted data is stored.</p> <div data-bbox="480 323 1041 841"> <p>This screenshot shows the PayPal login page. A Zoho Vault extension is open, displaying the user's email and password for 'a@gmail.com'. The password is shown in plain text, indicating it has been decrypted by the vault.</p> </div> <p>Source: Zoho user on Google Chrome</p> <div data-bbox="653 883 1434 1042"> <p>All passwords and other sensitive data that users store in Zoho Vault remain completely private and can only be viewed by the respective user. All user data gets encrypted and decrypted in the browser with the user's Zoho Vault master password, and only the encrypted data gets stored in Zoho's servers. The user's master password is never stored anywhere by Zoho Vault, meaning even Zoho can never access your data.</p> </div> <p>https://www.zoho.com/vault/security.html</p> <ul style="list-style-type: none"> • Decrypted user data (PayPal login credentials) – only available until the transaction is complete. • The decrypted/raw user data is removed from the temporary memory as soon as the transaction (CPU process) is over. <div data-bbox="1478 315 1980 886"> <p>This screenshot shows the PayPal login page. The Zoho Vault extension is open, but the password field is now filled with asterisks, indicating the data has been re-encrypted and is no longer in raw form.</p> </div> <p>Source: Zoho user on Google Chrome</p> <p>• Source: Zoho user on Google Chrome</p> <p>• https://www.zoho.com/vault/security.html</p>

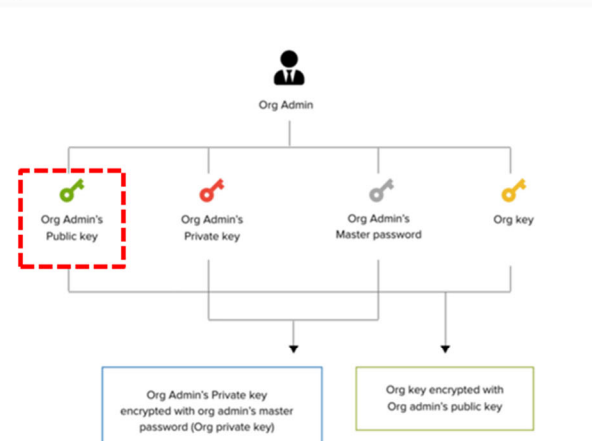
Claim Language	ZOHO Vault Applications
<p>2. The method of claim 1, wherein the detecting includes analyzing, by the browser toolbar, content of the web service to detect the request.</p>	<p>The Zoho Vault browser application can detect and analyze fields in a webform and fill them out with the appropriate user information. For example, it can tell if a field is asking for the user's name, email address, or password, and fill in that information accordingly without user's intervention.</p>  <p style="color: red; text-align: center;">Zoho Vault automatically fills appropriate fields with user information</p> <div style="display: flex; justify-content: space-around;"> <div data-bbox="676 662 1033 1055"> <p>See what's happening in the world right now</p> <p>Phone, email, or username Z</p> <hr/> <p>Password Z</p> <hr/> <p>Forgot password?</p> <p>Log in</p> <p>or</p> <p>Sign up</p> </div> <div data-bbox="1140 699 2001 1005" style="border: 1px solid black; padding: 5px;"> <p>\$ Auto Fill: If you are on the log-in page of a website or application and the related credentials have already been stored in Zoho Vault, you can just click the 'Auto Fill' button and then manually submit for auto-logon. Alternatively, if you right-click in the login page of any website whose credentials have already been stored with Zoho Vault, you will see Zoho Vault icon, which will show the list of passwords related to that site. You can click that and it will auto fill details.</p> <p>\$ You also have an option to copy usernames and passwords, so you can paste in some other place as required. Moreover, your passwords and related data are automatically synchronized every time you log in to the browser extension.</p> </div> </div> <div style="margin-top: 20px;"> <ul style="list-style-type: none"> • https://help.zoho.com/portal/en/kb/vault/user-guide/articles/vault-auto-log-in-to-websites#Using_the_Z-icon_from_the_login_fields • https://www.zoho.com/blog/vault/introducing-zoho-vault-browser-extensions-for-on-site-password-management.html </div>

Claim Language	ZOHO Vault Applications
<p>3. The method of claim 1, further comprising:</p> <p>authenticating, via the browser toolbar, the account holder prior to sending the request for the account information.</p>	<p>Zoho Vault requires a user to sign in before it will allow access to any account information stored on its servers. This ensures that only authorized users (“account holder”) can access sensitive user data.</p>  <p>https://accounts.zoho.com/signin?servicename=ZohoVault&signupurl=https://www.zoho.com/vault/signup.html&serviceurl=https://vault.zoho.com</p> <ul style="list-style-type: none"> • https://accounts.zoho.com/signin?servicename=ZohoVault&signupurl=https://www.zoho.com/vault/signup.html&serviceurl=https://vault.zoho.com

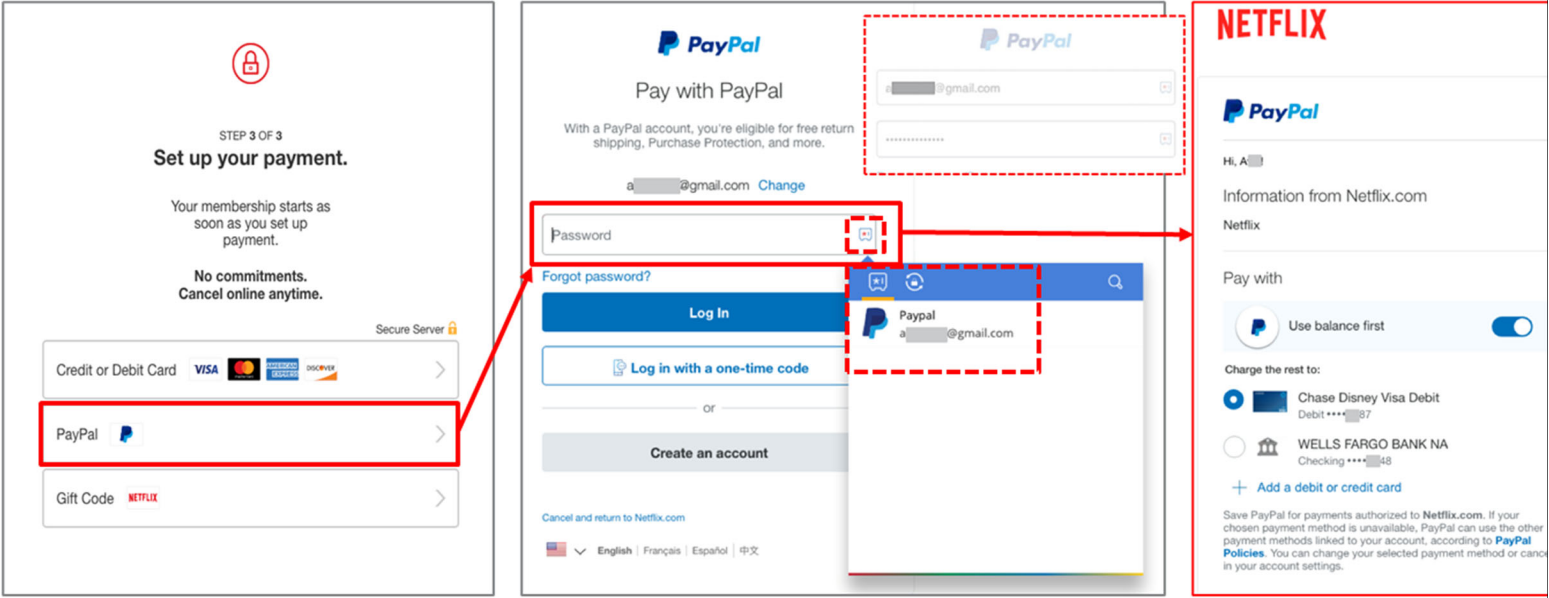
Claim Language	ZOHO Vault Applications
	<p>Zoho Browser application asks for the master password before accessing the menu of saved passwords.</p> <div data-bbox="499 289 1079 846"></div> <ul style="list-style-type: none">• <u>Source:</u> Zoho user on Google Chrome

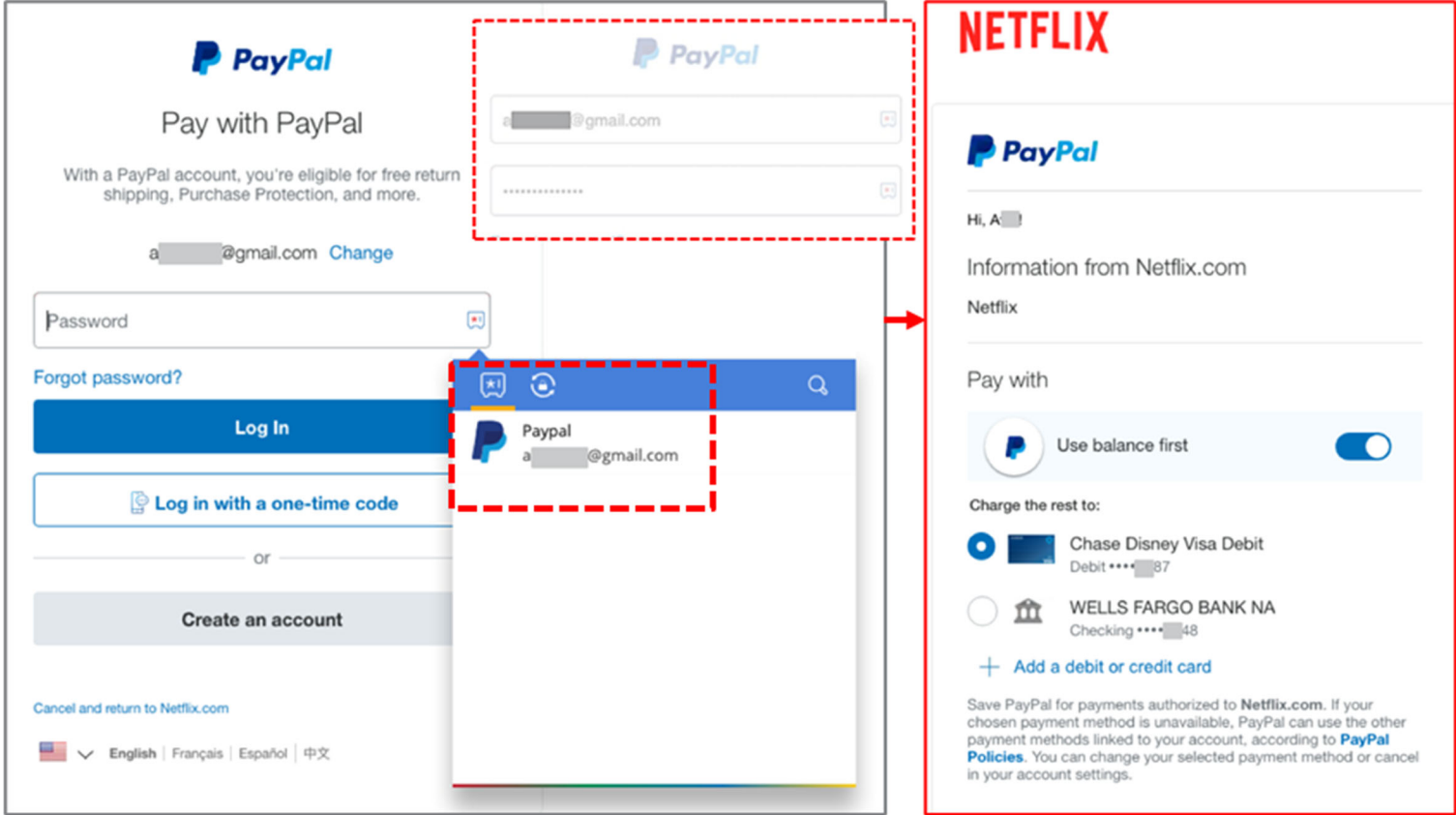
Claim Language	ZOHO Vault Applications
<p>5. The method of claim 1, wherein the removing is in response to closing a browser session with the web service.</p>	<p>Additionally, users have the option to end their browser session once they have completed a transaction. If a browser session connected to a web service is ended, the data will no longer be accessible in its unencrypted form.</p> <div data-bbox="541 289 1029 738"> <p>The screenshot shows the PayPal login page. A Zoho Vault extension overlay is visible, showing the user's email and password. The password is masked with dots. The extension is titled 'Paypal' and shows the email 'a@gmail.com'.</p> </div> <p>Source: Zoho user on Google Chrome</p> <div data-bbox="520 844 1192 982"> <p>All passwords and other sensitive data that users store in Zoho Vault remain completely private and can only be viewed by the respective user. All user data gets encrypted and decrypted in the browser with the user's Zoho Vault master password, and only the encrypted data gets stored in Zoho's servers. The user's master password is never stored anywhere by Zoho Vault, meaning even Zoho can never access your data.</p> </div> <div data-bbox="478 1039 1224 1073"> <ul style="list-style-type: none"> • https://www.zoho.com/vault/security.html • https://www.zoho.com/blog/vault/introducing-zoho-vault-browser-extensions-for-on-site-password-management.html </div> <div data-bbox="512 1198 1837 1351"> <ul style="list-style-type: none"> • Source: Zoho user on Google Chrome • https://www.zoho.com/vault/security.html • https://www.zoho.com/blog/vault/introducing-zoho-vault-browser-extensions-for-on-site-password-management.html </div> <div data-bbox="1108 310 1381 560"> <ul style="list-style-type: none"> • Decrypted user data (PayPal login credentials) – only available until the transaction is complete. • The decrypted/raw user data is removed from the temporary memory as soon as the transaction (CPU process) is over. </div> <div data-bbox="1402 280 1843 776"> <p>The screenshot shows the PayPal login page. A Zoho Vault extension overlay is visible, showing the user's email and password. The password is masked with dots. The extension is titled 'Paypal' and shows the email 'a@gmail.com'.</p> </div> <p>Source: Zoho user on Google Chrome</p> <div data-bbox="1312 833 1837 1006"> <ul style="list-style-type: none"> • holding passwords and other sensitive data as JavaScript variables (which cannot be accessed by any external application or other extensions), • storing other data in the background as local records and • passing credentials to websites. <p>Whenever the user logs out or remains idle for a specified time, local data gets completely erased.</p> </div>

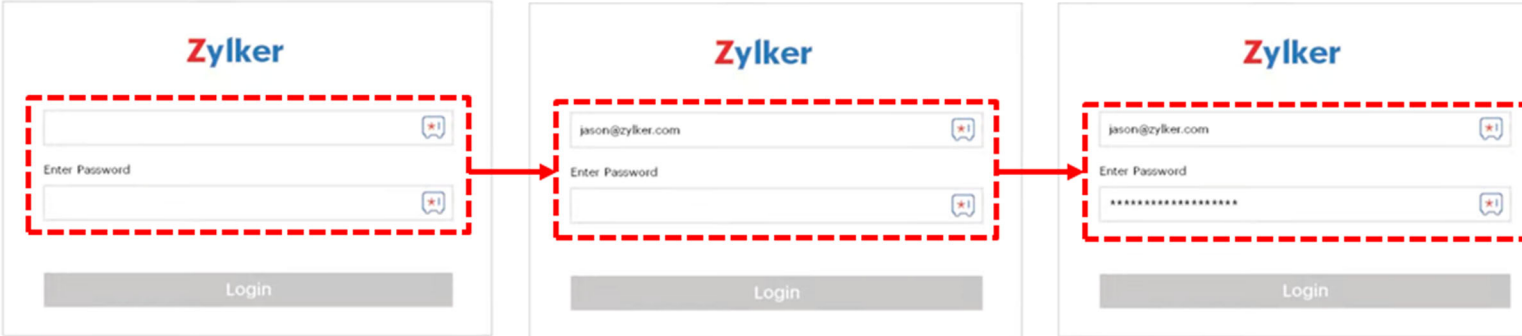
Claim Language	ZOHO Vault Applications
<p>6. The method of claim 1, further comprising:</p> <p>providing, via the browser toolbar, the stored account information to the web service in response to the detected request.</p>	<p>Zoho Vault automatically populates fields on a website with user account information (e.g., PayPal login information) in response to detected request.</p>  <p><u>Source:</u> Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription)</p> <p>https://www.zoho.com/vault/features/access-websites-with-a-single-click-browser-extension.html</p> <ul style="list-style-type: none"> • Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription) • https://www.zoho.com/vault/features/access-websites-with-a-single-click-browser-extension.html

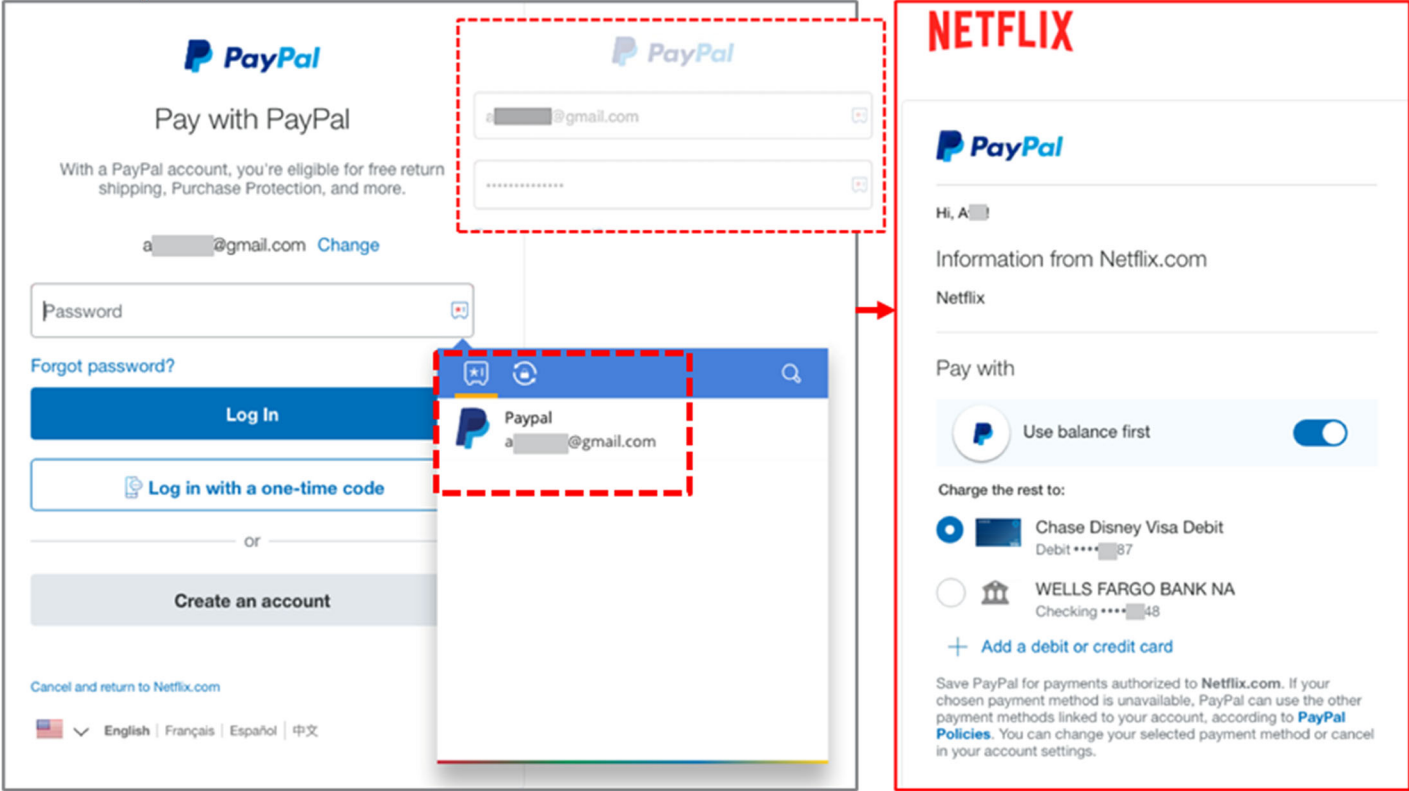
Claim Language	ZOHO Vault Applications
<p>7. The method of claim 1, further comprising:</p> <p>generating, via the browser toolbar, an encryption key pair, wherein the encryption key pair includes a public encryption key that corresponds to the encryption key.</p>	<p>Zoho Vault browser application generates an RSA Public-Private key pair.</p> <p>The "Private Key" is the key used to decrypt a user's account information. The "Public Key" is generated as a pair with the "Private Key" and corresponds to it.</p> <div data-bbox="483 357 1234 1023"> <p>When the org administrator signs up with Zoho Vault, an RSA Public-Private key pair is generated for them, along with an Org Key. This Org Key is an AES 256-bit key unique to every organization. The org admin's Private Key is encrypted using their master password and stored in Zoho Vault's database. Similarly, the Org Key is also encrypted using the org admin's RSA Public Key and stored in the database. Zoho Vault only stores the encrypted keys of the org admin's Private Key and Org Key. As per the host-proof-hosting model, the org admin's master password is not stored anywhere on the server. It remains only with the org admin.</p>  <p>Org Admin</p> <p>Org Admin's Public key</p> <p>Org Admin's Private key</p> <p>Org Admin's Master password</p> <p>Org key</p> <p>Org Admin's Private key encrypted with org admin's master password (Org private key)</p> <p>Org key encrypted with Org admin's public key</p> </div> <p>https://www.zoho.com/vault/security.html</p> <p>https://www.zoho.com/sites/default/files/zoho-vault-security-specifications.pdf</p> <p>An RSA public-private key is generated for each user during the sign-up process. A new org key (AES 256-bit) is also created for the organization during setup. The super administrator's private key is encrypted using the master password and is stored in our database. The org key is also encrypted using the super administrator's public key and stored in our database. During the handshake period, the encrypted org key stored in the database is decrypted using the super administrator's private key. The org key is then encrypted using the user's RSA public key and the newly encrypted org key is shared and stored in the user's database. When the user tries to share a password, the user's private key, which is stored in encrypted form in the database, is retrieved and decrypted using the user's master password. The newly encrypted org key shared by the super administrator is then retrieved. The encrypted org key is decrypted using the user's private key. The password to be shared is now encrypted using the org key.</p>
<p>15. A non-transitory computer readable medium having instructions stored thereon that are executable by a computer</p>	<p><i>ZOHO makes, uses, sells, offers for sale, and imports the Zoho Vault Applications via a non-transitory computer readable medium having instructions stored thereon that are executable by a computer system to cause the computer system to perform operations comprising the following.</i></p> <p><i>The same evidence that supports claim 1 also applies to claim 15.</i></p>

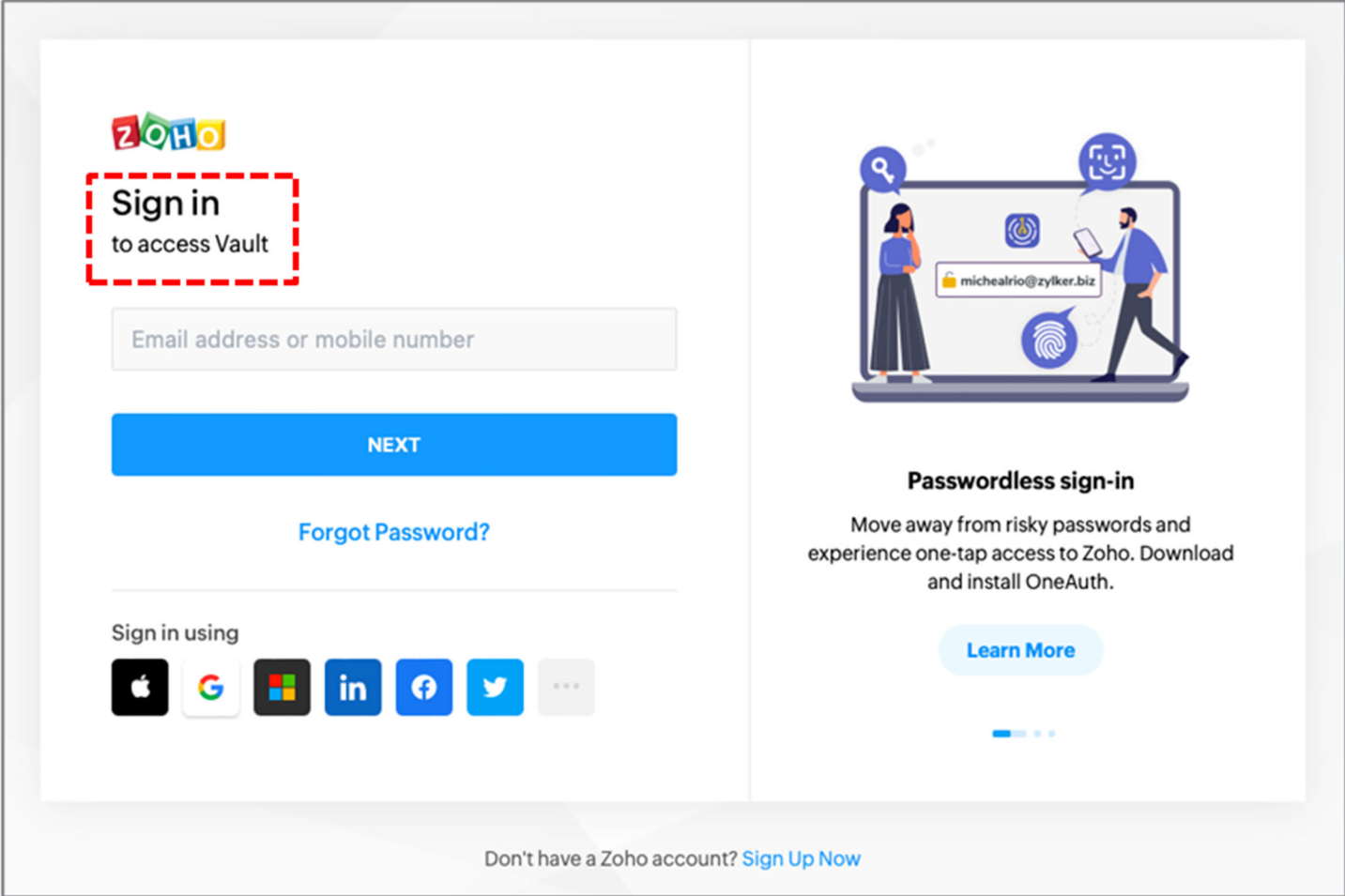
Claim Language	ZOHO Vault Applications
system to cause the computer system to perform operations comprising:	
determining, at a browser toolbar, that a request for account information has been received from a web service, wherein the account information is usable to conduct a transaction with an account holder;	<i>The same evidence that supports claim 1 also applies to claim 15.</i>
sending, via the browser toolbar, a request for the account information to a secure remote database;	<i>The same evidence that supports claim 1 also applies to claim 15.</i>
decrypting, at the browser toolbar, encrypted data received from the remote database to obtain the account information, wherein the decrypting is performed using an encryption key generated by the browser toolbar;	<i>The same evidence that supports claim 1 also applies to claim 15.</i>

Claim Language	ZOHO Vault Applications
<p>providing the account information to the web service to initiate the transaction; and</p>	<p>Zoho Vault provides user's login information for PayPal in order to initiate a payment transaction and obtain a Netflix subscription.</p>  <p>Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription)</p> <ul style="list-style-type: none"> • Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription)

Claim Language	ZOHO Vault Applications
<p>removing the account information from the computer system after providing the account information to the web service.</p>	<p>Zoho Vault does not store user's sensitive data unencrypted and removes it once a transaction is complete.</p> <p>As shown below, user's PayPal information is not available in unencrypted form once the user logs into PayPal successfully.</p>  <p>Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription)</p> <p>holding passwords and other sensitive data as JavaScript variables (which cannot be accessed by any external application or other extensions),</p> <ul style="list-style-type: none"> • Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription)

Claim Language	ZOHO Vault Applications
<p>16. The non-transitory computer readable medium of claim 15, wherein the determining includes analyzing, by the browser toolbar, web service content to detect the request from the web service.</p>	<p>The Zoho Vault browser application can detect and analyze fields in a webform and fill them out with the appropriate user information. For example, it can tell if a field is asking for the user's name, email address, or password, and fill in that information accordingly without user's intervention.</p>  <p style="color: red; text-align: center;">Zoho Vault automatically fills <u>appropriate fields</u> with user information</p> <div style="border: 2px solid red; padding: 10px; margin-top: 20px;"> <p>See what's happening in the world right now</p> <p>Phone, email, or username Z</p> <p>Password Z</p> <p>Forgot password?</p> <p>Log in</p> <p>or</p> <p>Sign up</p> </div> <div style="border: 1px solid gray; padding: 10px; margin-top: 20px;"> <p>\$ Auto Fill: If you are on the log-in page of a website or application and the related credentials have already been stored in Zoho Vault, you can just click the 'Auto Fill' button and then manually submit for auto-<u>login</u>. Alternatively, if you right-click in the login page of any website whose credentials have already been stored with Zoho Vault, you will see Zoho Vault icon, which will show the list of passwords related to that site. You can click that and it will auto fill details.</p> <p>\$ You also have an option to copy usernames and passwords, so you can paste in some other place as required. Moreover, your passwords and related data are automatically synchronized every time you log in to the browser extension.</p> </div> <ul style="list-style-type: none"> • https://help.zoho.com/portal/en/kb/vault/user-guide/articles/vault-auto-log-in-to-websites#Using_the_Z-icon_from_the_login_fields • https://www.zoho.com/blog/vault/introducing-zoho-vault-browser-extensions-for-on-site-password-management.html • https://help.zoho.com/portal/en/kb/vault/user-guide/articles/vault-auto-log-in-to-websites#Using_the_Z-icon_from_the_login_fields • https://www.zoho.com/blog/vault/introducing-zoho-vault-browser-extensions-for-on-site-password-management.html

Claim Language	ZOHO Vault Applications
<p>17. The non-transitory computer readable medium of claim 15, wherein the removing is performed in response to completion of the transaction.</p>	<p>Zoho Vault does not store user's sensitive data unencrypted and removes it once a transaction is complete.</p> <p>As shown below, user's PayPal information is not available in unencrypted form once the user logs into PayPal successfully.</p>  <p>Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription)</p> <p>holding passwords and other sensitive data as JavaScript variables (which cannot be accessed by any external application or other extensions),</p> <p>https://www.zoho.com/blog/vault/introducing-zoho-vault-browser-extensions-for-on-site-password-management.html</p> <ul style="list-style-type: none"> • Source: Zoho user on Google Chrome (performing PayPal transaction to obtain Netflix subscription) • https://www.zoho.com/blog/vault/introducing-zoho-vault-browser-extensions-for-on-site-password-management.html

Claim Language	ZOHOO Vault Applications
<p>20. The non-transitory computer readable medium of claim 15, wherein the operations further comprise:</p> <p>authenticating the account holder prior to sending the request to the secure remote database.</p>	<p>Zoho Vault requires a user to sign in before it will allow access to any account information stored on its servers. This ensures that only authorized users (“account holder”) can access sensitive user data.</p>  <p>https://accounts.zoho.com/signin?servicename=ZohoVault&signupurl=https://www.zoho.com/vault/signup.html&serviceurl=https://vault.zoho.com</p> <ul style="list-style-type: none"> • https://accounts.zoho.com/signin?servicename=ZohoVault&signupurl=https://www.zoho.com/vault/signup.html&serviceurl=https://vault.zoho.com